SECURE YOUR FIRM'S DATA:
Best Practices for Data Backup and Verification

frontline
MANAGED SERVICES

Cyber Security

Common ransomware prevention tools can help protect your Firm from an attack. Things like antivirus platforms, email filtering, pop-up blockers, and endpoint detection systems can significantly help protect from basic attacks. However, ransomware and cyber criminals can evade these measures with more and more ease, so it should not be considered a comprehensive solution. Criminals have adapted and now produce very sophisticated dupes that can trick even the most trained user, so a multi-layered approach is best for your Firm's security.

TIP: Establish and document a thorough cyber resiliency plan. It should document what to do before, during, and after an attack, including all steps and points of contact. This plan should be reviewed and updated regularly.

Business Continuity

Breaches can often result in considerable downtime and negative attention, since ransomware attacks are rarely limited to a single computer. The virus crawls for larger areas to compromise, such as servers and SaaS applications. Without a recovery and business continuity plan, nearly 20% of MSPs reported resolving to paying the ransom just to be able to return to business. Instead, your Firm's business continuity plan should include preparations such as:

- Hybrid cloud-based backup
- Automated backup processes
- Image-based backup processes
- Virtualization capabilities

TIP: Invite an IT Managed Service (ITMS) provider to audit your security system. Many ransomware attacks succeed because of unpatched systems, incorrect set-up in cloud systems like Microsoft 365, and a lack of filter services like VPNS. An ITMS provider can identify these weaknesses and develop a cost-efficient, scalable solution to bring your Firm back to best standing.

Have concerns or questions about your cybersecurity practices or your Firm's system?

Contact Frontline Managed Services for an audit and a discussion.